International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 2 | ISSN : 2456-3307

Privacy Preserving and Fine-Grained Data Access Control in Cloud Computing

S.Anto, S. Vimal, V.GuruMahesh
Computer Science and Engineering, Sri Krishna College of Technology, Coimbatore, TamilNadu, India

ABSTRACT

To real-time data security for petabytes of data is important for cloud computing. A recent survey on cloud security states that the security of users' data has the highest priority as well as concern. Therefore, this paper has developed a framework known as Cloud Computing Adoption Framework (CCAF) which has been customized for securing cloud data. CCAF is illustrated by the system design based on the requirements and the implementation demonstrated by the CCAF multi-layered security. Since our Data Center has 10 petabytes of data, there is a huge task to provide real-time protection and quarantine. We use Business Process Modeling Notation (BPMN) to simulate how data is in use. The use of BPMN simulation allows us to evaluate the chosen security performances before actual implementation.

Keywords : CCAF, BPMN, Data Center, SaaS, Data Protection

I. INTRODUCTION

Cloud Computing and its adoption has been a topic of discussion in the past few years. It has been an agenda for organizational adoption due to benefits in cost-savings, improvement in work efficiencies, business agility and quality of services. With the rapid rise in cloud computing, Software as a service (SaaS) is particularly in demand, since it offers services that suit users' need. Education as a service improves the quality of education and delivery. Mobile applications allow users to play online games and easy-to-use applications to interact with their peers. While more people and organizations use the cloud services, security and privacy become important to ensure that all the data they use and share are well protected. In this paper, we demonstrate our security design, implementation and solution for CCAF. We use penetration testing and related experiments to validate its robustness and measure precision, recall and F-measure to justify advantages over other approaches.

II. METHODS AND MATERIAL

File Upload

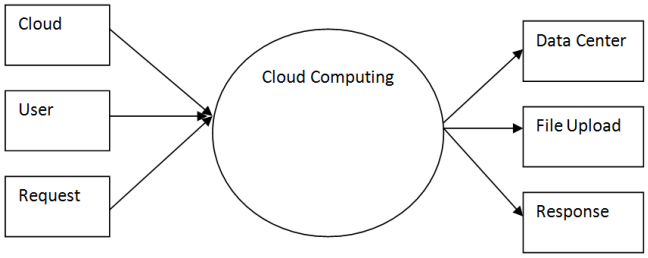
The entire files are converted into blocks; they are encrypted with the key, followed by signing the resulting encrypted blocks and creating the storage request. For each file, this key will be used to decrypt and rebuild the original file during the retrieval phase. The user also uses single sign-on to access each block with a compact signature scheme First, it can authenticate users during the storage/retrieval phase. Second, it can access control. Third, it can encrypt/decrypt data between users and their cloud.

Data Protection

This section describes the actions taken if Trojans and viruses are found. All malicious files and signatures are first isolated. The strong isolation and integrity management is used to protect user safety while using the CCAF security service. Strong isolation is required while detecting vulnerabilities in any of the cloud services, including the block of unauthorized IPs and attack points/ports. While these malicious files and unauthorized access attempts happen, quarantine is the next step to ensure the safety and security. It first backups the data safely and then attempts to quarantine infected data. If a quarantine action is unsuccessful, the

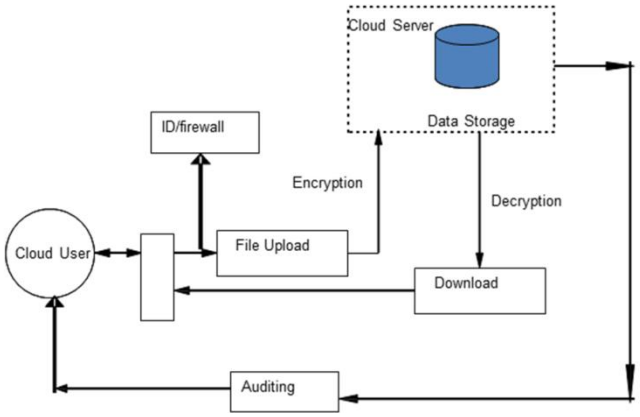
files can be kept under "quarantine area", or chosen to be deleted. In the quarantine area, the infected files are locked up until further no

Dataflow Diagram



SYSTEM ARCHITECTURE

EXISTING SYSTEM



They only provide an overview of important security challenges but do not provides full detailed solution on cloud security.There is no clear framework to be adopted to classify security requirements and then to feed towards implementation.Do not address in-depth data security issues, when the rapid growth of data is a challenge for the Data Center.A single solution is adopted to protect the data security and the data center.

III. RESULTS AND DISCUSSION

PROPOSED SYSTEM

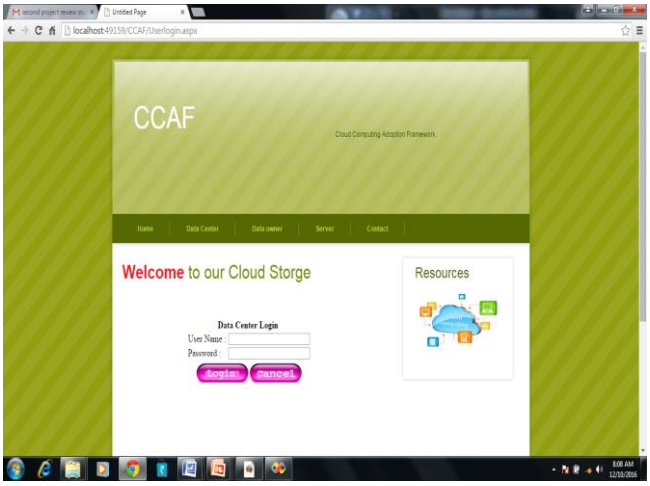
We proposed the multi-layered security to integrate security techniques to illustrate the essence and effectiveness of the framework with advantages of doing so. First, the strength of each technique is enhanced. Second, since each technique cannot always fully prevent hacking or provide a full solution without fallacy, the multi-layered security can improve the extent of security since it is more difficult for viruses and Trojans to break different types of security in one go. The aim is to maximize security protection and reduce the threats.To demonstrate the data security of the private clouds hosted in the data center, we propose the use of ethical hacking to demonstrate whether our CCAF multi-layered security can withstand a large amount of viruses and Trojans attacks, if the rapid data increase is from the external malicious hacking.

MODULE

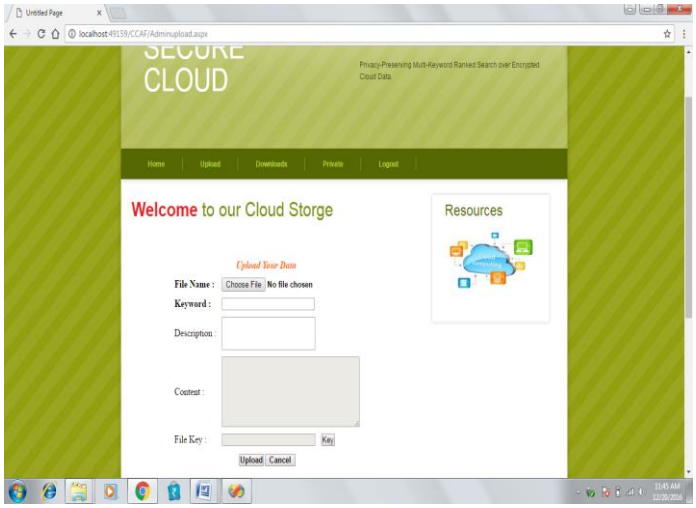
- Cloud User
- Data Center
- File Upload
- Data Protection

Cloud User

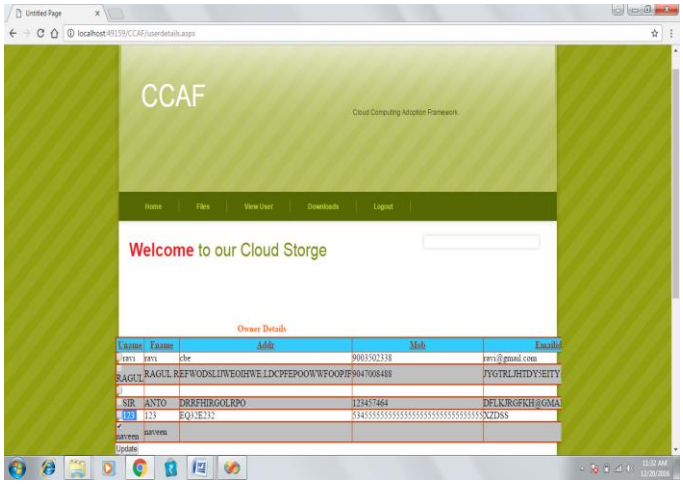
Data Center



File Upload



Data Protection



IV.CONCLUSION

Our paper has demonstrated the CCAF multi-layered security for the data security in the Data Center under the proposal and recommendation of CCAF guidelines. We explained the rationale, overview, components in the CCAF, where the design was based on the requirements and the implementation was illustrated by its multi-layered security. Our work can demonstrate that the use of CCAF multilayered security can protect the data center from the rapid data growth due to the security breach, and the use of BPMN can calculate how much time required for rescue action if the data security is compromised. In this way, we can work out the better tactics and plans for data recovery and security.

V. REFERENCES

[1] S. Marston, Z. Li, S. Bandyopadhyay, J. Zhang, and A. Ghalsasi, "Cloud computing – The business perspective," Decision Support Syst., vol. 51, no. 1, pp. 176–189, 2011.

[2] M. A. Vouk, "Cloud computing—issues, research and implementations," J. Comput. Inf. Technol.—CIT, vol. 4, pp. 235–246, 2008.

[3] A. K. Jha, C. M. DesRoches, E. G. Campbell, K. Donelan, S. R. Rao, T. G. Ferris, and D. Blumenthal, "Use of electronic health records in US hospitals," New England J. Med., vol. 360, no. 16, pp. 1628– 1638, 2009.

[4] H. T. Peng, W. W. Hsu, C. H. Chen, F. Lai, and J. M. Ho, "Financial cloud: open cloud framework of derivative pricing," in Proc. Int. Conf. Social Comput., Sep. 2013, pp. 782–789.

[5] G. McGraw, Software Security: Building Security. Reading, MA, USA: Addison-Wesley, 2006.

[6] P. Brooks and J. Chittenden, Metrics for Service Management: Designing for ITIL. Zaltbommel, Netherlands: Van Haren Publishing, 2012.

[7] V. Chang, R. J. Walters, and G. Wills, Cloud Storage and Bioinformatics in a Private Cloud Deployment: Lessons for Data Intensive Research. New York, NY, USA: Springer CLOSER 2012, CCIS 367, pp. 245–264, 2013.

[8] V. Chang, "Business intelligence as service in the cloud," Future Gener. Comput. Syst., vol. 37, pp. 512–534, 2014.